MONTANA

INFORMATION SECURITY (INFOSEC)

Program

BASIS : MONTANA CODE ANNOTATED (MCA 2-15-114 AND MCA 2-17-534)

MODEL : NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION 800-39 MANAGING INFORMATION SECURITY RISK (ORGANIZATION, MISSION, AND INFORMATION SYSTEM VIEW)

Framework for addressing Information Security through Risk Management from an “*Enterprise*” or “Business” approach.

INFOSEC – BASIS

- Montana Code Annotated.
- 2-15-114 Each department head is responsible for ensuring an adequate level of security for all data within that department.
- Extends beyond just Information Technology-includes business application.
- Includes requirement for efficiency with economic initiatives-budget requirements.

INFOSEC – MODEL

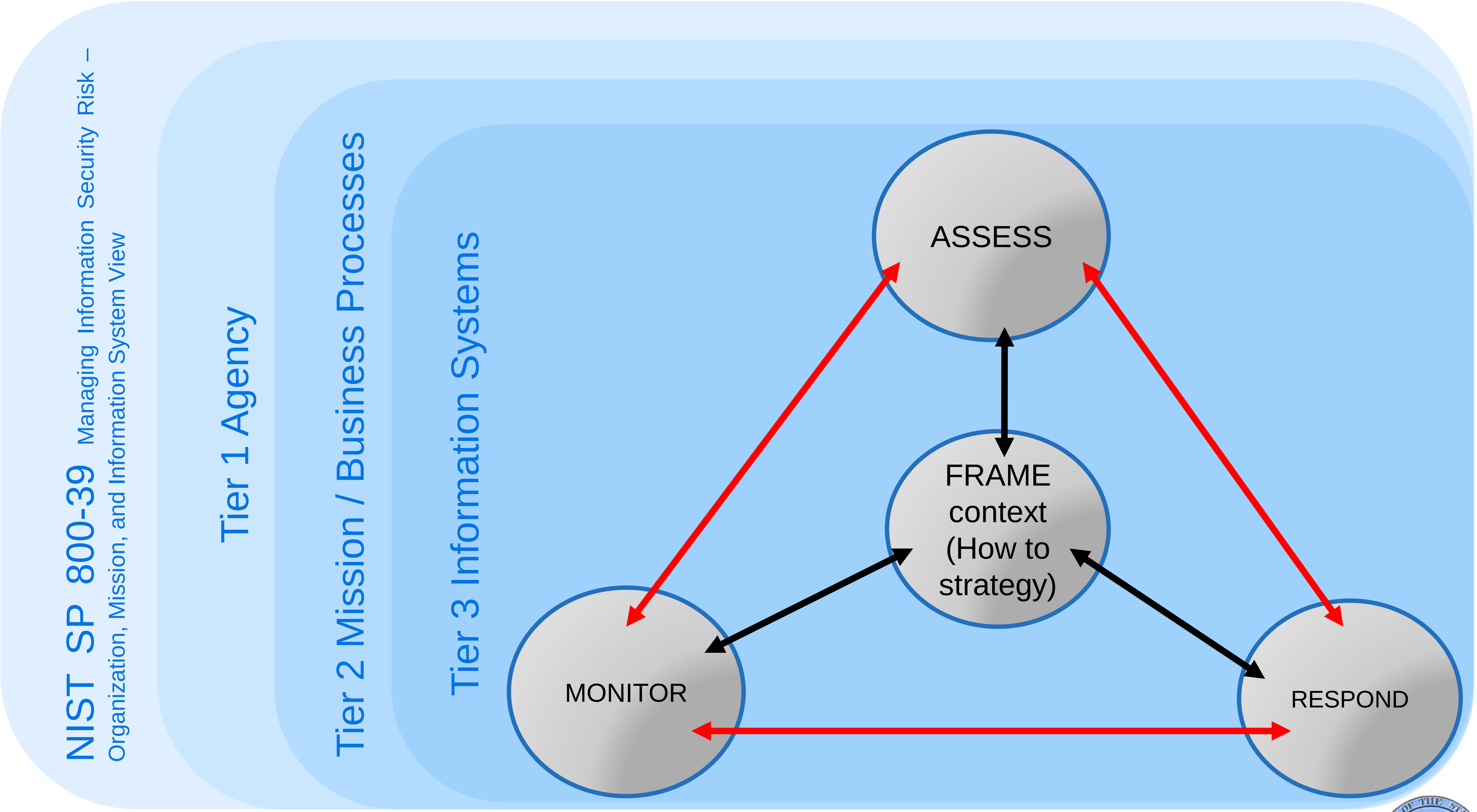
- Montana has chosen the NIST Special Publication 800-39 as the business model of choice for institutionalizing a process for Information Security (Policy 1240.X08 Information Security Programs effective July 1, 2012).
- This model is consistent with Change and Quality Management Business principles for continuous improvement.

INFOSEC – A WAY AHEAD

- A team approach through an institutionalized integrated structure …
  - ➢ Agencies-the executive branches of state government
  - ➢ Information Security Policy Analyst, DoA-SITSD Position
  - ➢ ISMG
  - ➢ ITMC
  - ➢ ITB

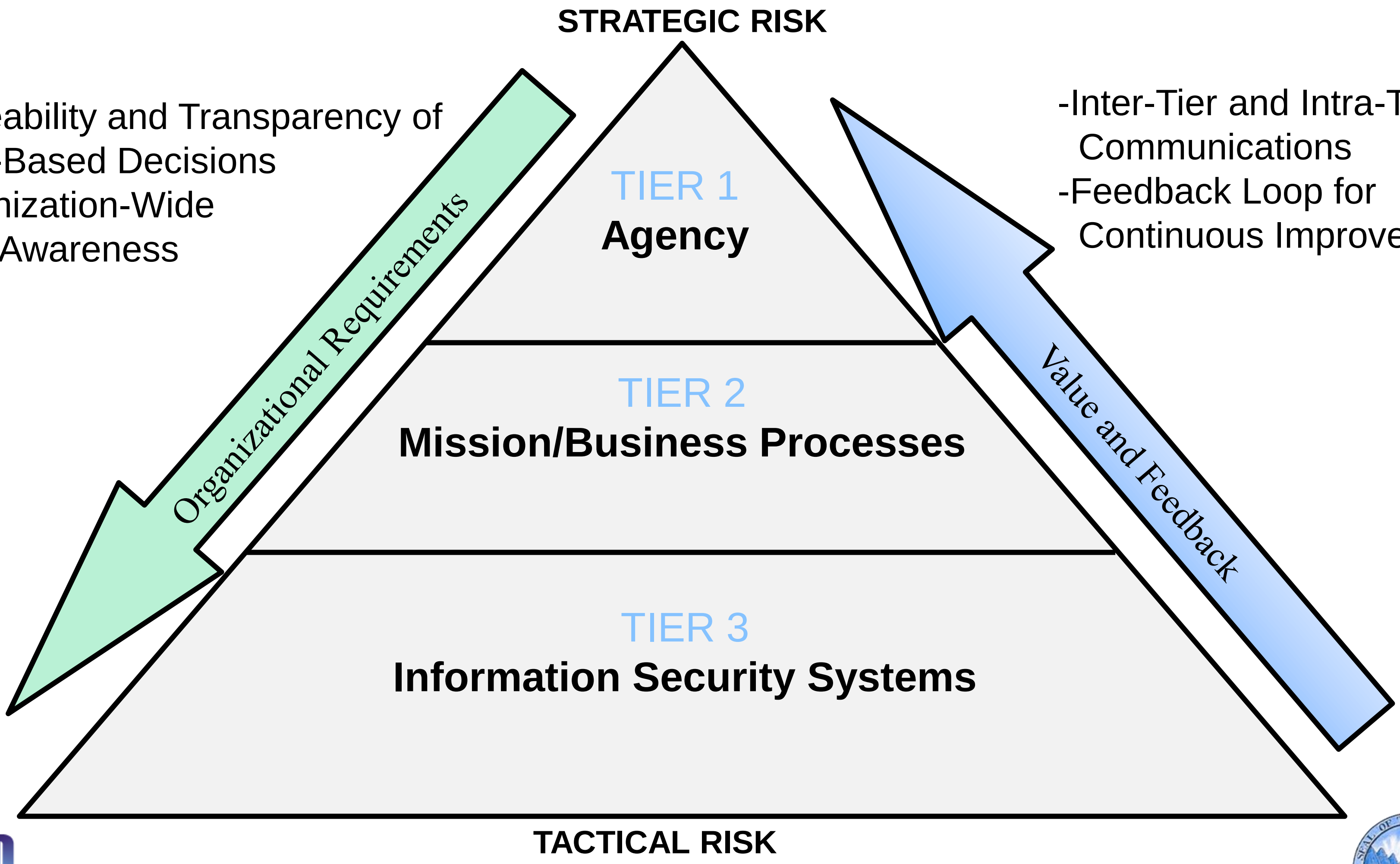
Risk Management Process

(Information and Communication Flow Components and Levels)



NIST SP 800-39 Managing Information Security Risk – Organization, Mission, and Information System View
Tier 1 Agency
Tier 2 Mission / Business Processes
Tier 3 Information Systems
ASSESS
FRAME context (How to strategy)
MONITOR
RESPOND

Multi-tiered Enterprise-Wide Risk Management Strategy



STRATEGIC RISK

-Traceability and Transparency of Risk-Based Decisions

-Organization-Wide Risk Awareness

Organizational Requirements

TIER 1

Agency

TIER 2

Mission/Business Processes

TIER 3

Information Security Systems

Value and Feedback

-Inter-Tier and Intra-Tier Communications

-Feedback Loop for Continuous Improvement

TACTICAL RISK

The Road Map has begun…

- Build the enterprise “Information Risk Management Strategy” template.
- Facilitate completed Information Security Plans for each Agency by 1 July 2012.
- Assist procurement with contract language to address INFOSEC for contractor responsibility when handling sensitive state or personal information.
- Further define interaction between stakeholders towards desired end-state.
- Complete a proposed integration system that addresses all aspects of INFOSEC by 31 Dec 2012.

Desired End-State, Jan 2013

- Institutionalized INFOSEC program capable of meeting need for change to deal with continuous challenges from technological advances, human factors, and evolving requirements.
- Integrated INFOSEC program between all Agencies, Processes and Programs that interact with, manage, or process information, data, and records.
- Enterprise compliance with legal and regulatory requirements.